UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,827	12/21/2005	Michael Jacobs	CHAP-005	3097

36822 7590 03/04/2009

GORDON & JACOBSON, P.C.
60 LONG RIDGE ROAD
SUITE 407
STAMFORD, CT 06902

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,827	JACOBS, MICHAEL	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *43-62* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *43-62* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to Amendment filed 12/15/2008.

2. Claims 24-42 cancelled. Claims 43-62 are new. Claims 43-62 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 43-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh et al. (US Patent Publication No. 2002/0004902 and Toh hereinafter) in view of Haber et al. (US Patent No. 5,781,629 and Haber herenafter).

4. As to claim 43, Toh teaches a method of permitting authentication of data comprising: (a) storing copies of a plurality of data items (e.g., … local storage [par. 36]); (b) generating a first data file (e.g., data package) comprising a respective hash value of each said plurality of stored data items (i.e., …teaches sending an original data package as well as it encrypted hash [par. 58]); (c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items (i.e., … teaches creating a hash of original data package [par. 58]) ; (d) transmitting said single hash value to a remote location (e.g., Operation Center) (i.e.,

… teaches sending encrypted hash of the data package to Operation Center [par. 58]), via an information technology communications network [fig. 2];

Toh does not teach:

(e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value; (f) generating a hash value for said second data file; and (g) publishing said hash value for said second data file in a journal for authenticating said second data file.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses:

(e) creating at said remote location (e.g., service bureau) a second data file comprising said single hash value and one or more additional data items relating to said single hash value (to provide the capability to create a second document (e.g., second data file) at a remote location [col. 5, lines 44-48]);

(f) generating a hash value for said second data file (to provide the capability to generate a hash value for the second document [col. 5, lines 45-50]).

(g) publishing said hash value for said second data file in a journal for authenticating said second data file (to provide the capability to publish a hash value [col. 6, lines 45-60]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by

employing the well known feature of published Hash values as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 6, lines 45-60].

2. As to claim 44, Toh teaches a method further comprising: (h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in (g) (i.e., … teaches authentication by comparing hashes [par. 67]).

Toh does not teach the claim limitation element of generating a second hash value of a second document (e.g., second data file). However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: generating a hash value for said second data file (to provide the capability to generate a hash of a second document (e.g., second data file) [col. 5, lines 45-50]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of generating a hash value of a second document as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 5, lines 45-50].

2. As to claim 45, Toh teaches a method where said first data file is generated in (b) at the end of a predetermined time period (par. 86).

5. As to claim 46, Toh teaches a method where: said first data file (e.g., delivery) contains at least one identifier selected from the group consisting of a file name, a path name, a file size and a time stamp (i.e., ... teaches delivery content including header information (e.g., address information) [par. 67]).

6. As to claim 47, Toh teaches a method further comprising: (i) generating a hash value for a selected one of the data items [par. 58]; (j) digitally signing and encrypting said hash value with a secret identifier associated with the first user; (k) transmitting to a second user said encrypted hash value (i.e., .. teaches sending encrypted Hash of the data package [par. 58]; and generating a further hash value for said received encrypted hash value [par. 58]; (m) encrypting the further hash value with a private identifier associated with a second user (i.e., … teaches creating a digest or hash number and further encrypting the hash number or digest with the sender private key [par. 67]); (n) encrypting the encrypted further hash value with a public identifier associated with the first user (par. 67); and (o) returning the encrypted further hash value of (n) to the first user (i.e., ... teaches sending the encrypted hash value [par. 67]).

Toh does not teach the claim limitation element of receiving and storing said transmitted encrypted hash value for audit purposes; However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: receiving and storing said transmitted encrypted hash value for audit purposes (to provide the capability to receive and store hash values [col. 13, lines 50-60]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of receiving and storing Hash values as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 13, lines 50-60].

7. As to claim 48, Toh teaches a method further comprising: (p) receiving said encrypted further hash value of (n) returned to the first user in step (o) (i.e., … teaches encrypting hash value [par. 67] (q) decrypting said received encrypted data with the private identifier associated with said second user and the public identifier associated with said first user to derive a hash value therefrom (i.e., ... teaches receiving encrypted data and decrypting encrypted using public key to obtain a hash [par. 67]; and (r) comparing the hash value derived in (q) with the hash value generated in (j) to confirm digital identity of the second user (i.e., … teaches comparing hash values for purposes of authentication [par. 67]).

Toh does not teach the claim limitation element of receiving said transmitted encrypted hash value; However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: receiving said transmitted encrypted hash value (to provide the capability to receive and store hash values [col. 13, lines 50-60]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of receiving Hash values as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 13, lines 50-60].

8. As to claim 49, Toh teaches a method further comprising: (s) in response to the comparing of (r) confirming digital identity (e.g., strong authenticaiton) of the second user (i.e., ... teaches a receiving system strongly authenticates to the OC [par. 70]), encrypting the secret identifier (e.g., decryption key) associated with the first user and transmitting to the second user the encrypted secret identifier associated with the first user for decryption and subsequent use in decrypting said encrypted data item of [par. 66].

9. As to claim 50, Toh teaches a method according further comprising: in response to the comparing of (r) failing to confirm digital identity of the second user, denying the second user access to the encrypted data item of (i.e., ... teaches user authentication (par. 67)).

10. As to claim 51, Toh teaches method where the second user is denied access to the encrypted data item of by omission of transmitting to the second user the encrypted secret identifier (e.g., document decryption key) associated with the first user (i.e., … teaches revocation prevent communication [par. 50]).

11. As to claim 52, Toh teaches a method where: the encrypted secret identifier (e.g., document decryption key) generated is encrypted with a key that is obtained through a transaction between said second user and a third party (i.e., … teaches obtaining from OC a public key to encrypt a decryption key [par. 66]).

12. As to claim 53, Toh teaches a method where: said transaction between said second user and said third party is recorded and time stamped by said third party (e.g., OC) (i.e., ... teaches for tracking purposes the OC maintains a delivery timestamp [par. 85]0.

13. As to claim 54, Toh teaches a method of transmitting data between a first user and a second user via an information technology communications network, comprising the steps of: generating a first hash value for a selected one of the data items (par. 67);

digitally signing and encrypting said first hash value with a secret identifier associated with the first user (i.e., ... teaches digitally signing [par. 59] ... further teaches encrypting the hash value [par. 67]);

transmitting to a second user said encrypted first hash value (par. 67);

encrypting the second hash value with a private identifier associated with a second user and a public identifier associated with the first user (par. 67);

Toh does not teach:

receiving and storing said transmitted encrypted first hash value for audit purposes and generating a second hash value for said received encrypted first hash value;

encrypting the second hash value with a private identifier associated with a second user and a public identifier associated with the first user; and returning the encrypted second hash value to the first user.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses:

receiving and storing said transmitted encrypted first hash value for audit purposes and generating a second hash value for said received encrypted first hash value (to provide the capability to generate a hash value for the second document [col. 5, lines 45-50 & col. 13, lines 50-60);

and returning (e.g., publish) the encrypted second hash value to the first user (to provide a second hash [col. 7, lines 20-30]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of published Hash values as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 6, lines 45-60].

14. As to claim 55, Toh teaches a method further comprising: receiving said encrypted second hash value returned to the first user (par. 67);

decrypting said received encrypted second hash value with the private identifier associated with said second user and the public identifier associated with said first user to derive a hash value therefrom (par. 67);

and comparing the derived hash value derived with the second hash value generated for said received encrypted first hash value to confirm digital identity of the second user (i.e., … teaches authentication by comparing hashes [par. 67]).

Toh does not teach the claim limitation element of generating a second hash value of a second document (e.g., second data file). However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: generating a hash value for said second data file (to provide the capability to generate a hash of a second document (e.g., second data file) [col. 5, lines 45-50]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of generating a hash value of a second document as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 5, lines 45-50].

.

15. As to claim 56, Toh teaches method further comprising: in response to the comparing of confirming digital identity of the second user, encrypting the secret identifier associated with the

first user and transmitting to the second user the encrypted secret identifier associated with the first user for decryption and subsequent use in decrypting said encrypted first hash value [par. 67].

16. As to claim 57, Toh teaches a method further comprising: in response to the comparing of failing to confirm digital identity of the second user, denying the second user access to the encrypted first hash value (i.e., ... teaches user authentication (par. 67)).

17. As to claim 58, Toh teaches a method where the second user is denied access to the encrypted first hash value by omission of transmitting to the second user the encrypted secret identifier associated with the first user (i.e., … teaches revocation to prevent communication [par. 50]).

18. As to claim 59, Toh teaches method where the secret identifier is encrypted with a key that is obtained through transactions between said second user and a third party (e.g., OC) [par. 72].

19. As to claim 60, Toh teaches a method where: at least one of said transactions between said second user and said third party is recorded and time stamped by said third party [par. 85].

20. As to claim 61, Toh teaches method where the encrypted first hash value is stored remotely from said first and second end users (i.e., ... teaches encrypting a hash value [par. 67]).

Toh does not teach the claim limitation element of storing the hash remotely. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: storing the hash remotely (to provide the capability to receive and store hash values [col. 13, lines 50-60]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of storing the Hash values as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 13, lines 50-60].

21. As to claim 62, Toh teaches a method where the encrypted first hash value is stored by a third party (i.e., ... teaches encrypting a hash value [par. 67]).

Toh does not teach the claim limitation element of storing a hash with a third party. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: storing the hash with a third party (to provide the capability to store hash values with a third party (e.g., service bureau) [col. 13, lines 50-60]).

Therefore, given the teachings of Haber, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh by employing the well known feature of storing a Hash values as disclosed above by Haber, for which data transaction authentication and storage will be enhanced [col. 13, lines 50-60].

Response to Arguments

Applicant's arguments with respect to claims 43-62 have been considered but are moot in view of the new ground(s) of rejection. The new rejection is under the combined teachings of Toh in view of Haber. With regards to applicant's primary argument concerning "**published hash values**", Examiner contends applicant's argument is moot under the new rejection of Toh and Haber. Examiner cites the specific teachings of Haber, for which recites the capability to link and publish hash values (col. 6, lines 46-52).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on

the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435